DATA SHEETS

XONA Critical System Gateway (CSG)

+1 866-849-6629 | info@xonasystems.com

GET IN. GET TO WORK. GET IT DONE.

DELIVERING UNMATCHED ZERO-TRUST SECURE USER ACCESS WITHOUT DISRUPTIONS

The XONA Critical System Gateway (CSG) is purpose-built to provide frictionless and compliant user access to critical infrastructure (CI) and operational technology (OT) assets. XONA enables simple and secure remote operations to these CI and OT assets while protecting them from cyber threats posed by a distributed workforce including third parties. The CSG allows users to quickly connect and manage critical infrastructure assets and systems from anywhere at any time.

ENABLING SECURE REMOTE OPERATIONS

The XONA CSG brings secure remote operations to operational technology and other critical infrastructure assets while reducing the dependency on less secure, complex, and outdated legacy technologies such as VPNs and Jump Servers.

XONA is trusted by leaders in the chemical, energy, food & beverage, government, industrial machinery, manufacturing, oil & gas, renewables, and transportation industries.

ACCOMPLISHING SCALABLE SECURE USER ACCESS

The XONA platform has integrated a zero-trust framework comprised of multi-factor authentication, user-to- asset access controls, protocol isolation, user session analytics, and automatic video recording. Support for SAML 2.0 is available. XONA is the single, secure portal to the cyber-physical world enabling critical operations to happen from anywhere at any time with total confidence and trust.

PROTOCOL ISOLATION DELIVERS UNPRECEDENTED SECURITY & USER ACCESS

XONA's proprietary Protocol Isolation effectively breaks the cyber kill chain, dramatically reducing the network's attack surface. XONA prevents the exposure of protocols on an untrusted network such as the internet while giving authorized users seamless and secure control of operational technology from any location or device. XONA takes the protocols on the trusted network and translates them to an interactive video stream that only requires port 443 open to the untrusted network. XONA's approach means that you can replace legacy technologies (e.g., RDP, VPNs, Jump Servers, etc.) and insecure workarounds used to grant users access to the trusted network with a proven high-availability zero-trust solution.

BENEFITS

Zero-Trust Architecture

Rely on XONA's underlying zero-trust model for simple and secure authentication (SAML 2.0 supported) and a 'least privilege' approach to authorization that only allows access to approved assets/devices.

Clientless, Agentless and Browser-based

Quickly access and operate critical assets in real-time through XONA CSG from any device with a standard web browser—no plug-ins, agents, or clients necessary.

Compliance

XONA features map to zero- trust architecture for explicit authorization and authentication and supports NERC CIP, IEC 62443 and NIST 800-53 compliance standards.

Moderated Access and Secure File Transfer

Safeguard against data theft through XONA's unique supervisory approval process, including wait lobby for site-level access to CI assets and directional-based file transfer for protected critical assets.

Purpose-Built for OT & Critical Infrastructure

Connect in seconds, users work in real-time, on-premise hardware or virtual appliances available with no cloud or "phone-home" dependencies, user and asset segmentation and isolation, and support for secure third-party vendor access including Just-in-time (JIT) controls.

User Access - Read-Only Monitoring

Facilitate CI and OT asset troubleshooting and training through "over the shoulder" support to CI operational procedures with read- only monitoring of technician access in the control room.

Multi-Factor Authentication (MFA)

Seamlessly authenticate with WebAuthn, U2F, or OTP compliant hardware tokens, TOTP compliant mobile app, or integrate with your legacy MFA solution.

User Access Logging and Recording

Get a firsthand look into every user's actions with detailed user access and event logs, plus user session screen recording.

Protocol Isolation

Securely stream applications and convert remoting protocols into an encrypted display presented in any browser.

ZERO TRUST WITH SECURITY-FIRST APPROACH

Helps address shadow IT, insecure workarounds (I.e., risky password sharing). Delivers session moderation & auditing, Zero Trust by design, mature integrations & APIs, secure boot, dramatically reduces the network attacks surface, and breaks the cyber kill chain for malware and ransomware attacks.

MEETING & STAYING COMPLIANT

Depend on an efficient, cost-effective platform to address NERC, IEC, and NIST requirements and standards. XONA utilizes protocol and system isolation, encrypted display, multi-factor authentication, session logging, and recording of user access to support compliance requirements that secure against cybersecurity risks.

Zero-Trust Architecture

XONA has been third-party tested and complies fully with NERC CIP Cybersecurity Standards 005-5, 007-6, 003-9, 011-2 and 013-1.

Learn More

Clientless, Agentless and Browser-based

XONA provides security capabilities to meet the requirements of the 62443 standards about access control, identification, and authentication control, use control, data confidentiality, and least privilege.

Learn More

Compliance

XONA provides key capabilities to meet NIST 800-53 and FIPS 140- 2. XONA employs standards-based and FIPS validated crypto libraries such as Libgcrypt and Open SSL.

OPERATIONAL BENEFITS

XONA has no dependencies on “phoning home” or cloud access to operate, including no network reconfigurations. XONA is browser-based and does not require agents, cloud, or the installation of a native software client. XONA’s proprietary protocol isolation and zero-trust approach significantly reduces the technology footprint, system administration, and staff. XONA can also help eliminate redundant technology (e.g., jump servers, VPNs) that introduce complexity, overhead, and cyber risk into accessing and operating critical systems.

DEPLOYMENT FLEXIBILITY

OT and critical infrastructure operate under strict security, safety, and compliance requiring unique deployment and configuration options to strengthen and provide secure operational access to these systems. XONA has flexible deployment options that install in less than 30-minutes and allows for rapid provisioning that is easy to use and manage.

1U & Din Rail

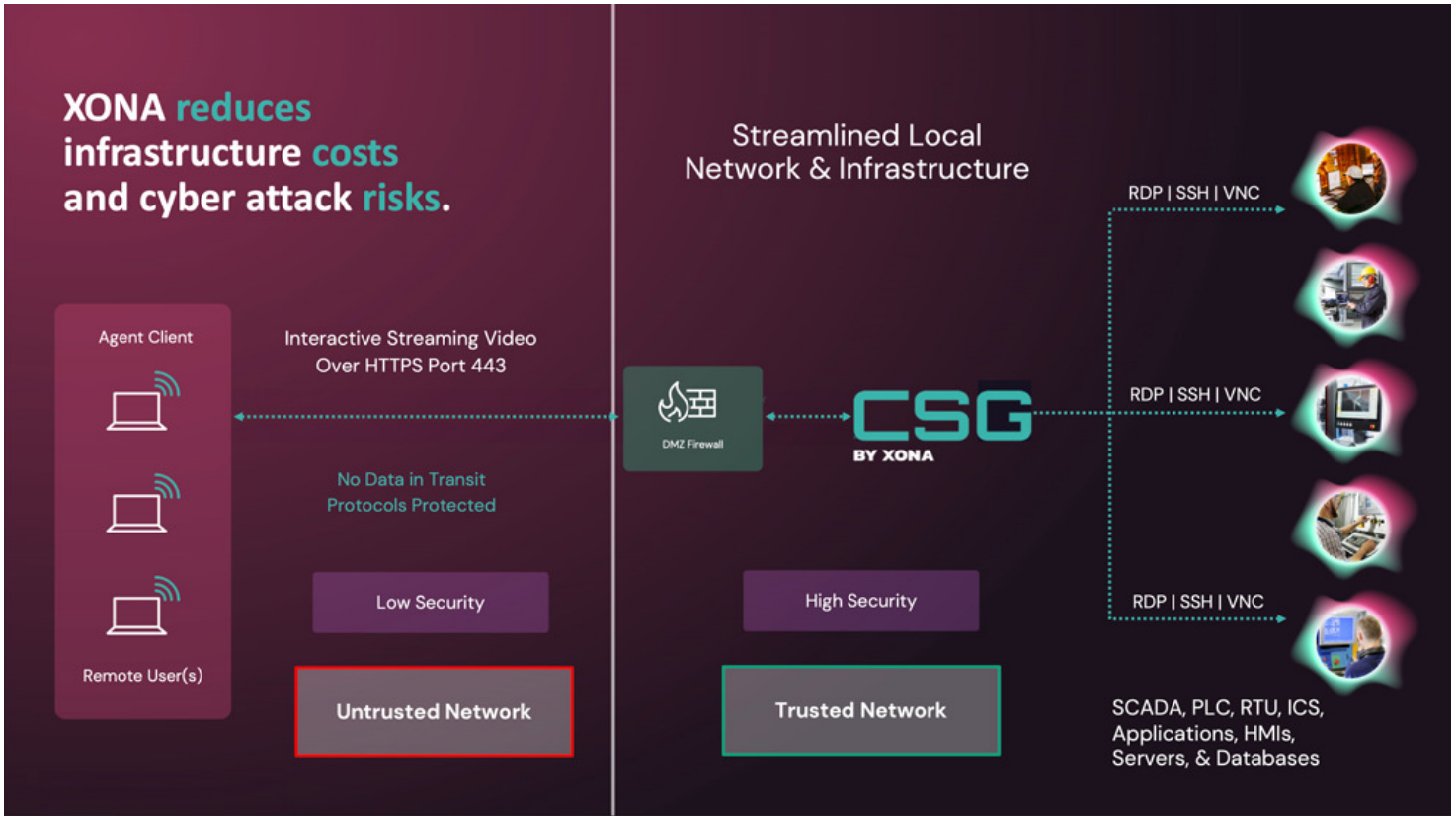
XONA supports standard 1U and DIN Rail form factors including robust Industrial Design compliant with IEC61850 and IEEE 1613 standards.

PARA-Pack

Whether it's a remote, isolated, disaster recovery, or an internet outage, the CSG Para-Pack enabled users to securely connect to these remote networks and their assets using a cellular network to connect to the on-site CSG.

Virtual Machine/Appliance

XONA can be deployed as a virtual appliance on major hypervisors.



+1 866-849-6629 | info@xonasystems.com

ABOUT XONA

XONA enables frictionless user access that's purpose-built for operational technology (OT) and other critical infrastructure systems. Technology agnostic and configured in minutes, XONA's proprietary protocol isolation and zero-trust architecture immediately eliminates common attack vectors, while giving authorized users seamless and secure control of operational technology from any location or device. With integrated MFA, user-to-asset access controls, user session analytics, and automatic video recording, XONA is the single, secure portal that connects the cyber-physical world and enables critical operations to happen from anywhere with total confidence and trust.

+1 866-849-6629 | info@xonasystems.com